Οικονομική εγκληματικότητα και νέες τεχνολογίες: Ηλεκτρονικές απάτες

Μαρία Κράνη

19/11/2020

Figure 1. Πηγή εικόνας: unshplash.com

Εισαγωγή

Η εξέλιξη της τεχνολογίας έχει συμβάλλει, μεταξύ άλλων, στη διευκόλυνση της επικοινωνίας και της πληροφόρησης, ενώ παράλληλα είναι προσβάσιμα εύκολα στην πλειοψηφία του πληθυσμού. Ωστόσο, παρά τα πολλά πλεονεκτήματα της, ενέχει πολλούς και σημαντικούς κινδύνους. Όσον αφορά στην εγκληματικότητα, η συμβολή των νέων τεχνολογικών μέσων και του διαδικτύου είναι μεγάλη. Έτσι, συχνά παρατηρούμε την εμφάνιση νέων μορφών εγκληματικότητας που χρειάζονται την βοήθεια της τεχνολογίας για τη διάπραξή τους, ή ακόμα και παραδοσιακές μορφές

εγκληματικότητας, οι οποίες υποβοηθούμενες από τα σύγχρονα τεχνολογικά μέσα, αλλάζουν χαρακτήρα, δομή, μορφή ή περιεχόμενο. Με το παρόν άρθρο, επιχειρείται η εξέταση μιας παραδοσιακής μορφής εγκληματικότητας, της οικονομικής εγκληματικότητας, στο πλαίσιο των νέων τεχνολογιών. Συγκεκριμένα, γίνεται αναφορά σε μια κατηγορία ηλεκτρονικού-οικονομικού εγκλήματος, τις ηλεκτρονικές απάτες, καθώς και στην αντιμετώπισή της σε θεσμικό πλαίσιο, σε διεθνές επίπεδο.

1. Εννοιολογικός προσδιορισμός της οικονομικής εγκληματικότητας στο διαδίκτυο

Η διατύπωσε ενός μοναδικού ορισμού για το οικονομικό έγκλημα αποτελεί ένα εξαιρετικά δύσκολο εγχείρημα, καθώς αφορά σε μια πληθώρα παράνομων πράξεων. Ωστόσο, μπορούμε να επισημάνουμε ότι με τον όρο «οικονομικό έγκλημα» αναφερόμαστε σε μία κατηγορία πράξεων που λαμβάνουν χώρα στο πλαίσιο της αγοράς, θίγουν έννομα αγαθά που έχουν σχέση με το οικονομικό σύστημα και αποτελούν παραβιάσεις νόμων που ρυθμίζουν τις εσωτερικές λειτουργίες της αγοράς και τις σχέσεις της με την ευρύτερη κοινωνία (Λάζος, 2004).

Ο πρώτος που μίλησε για την οικονομική εγκληματικότητα και μάλιστα συνδέοντας την με τις υψηλότερες κοινωνικοοικονομικές τάξεις ήταν ο Αμερικάνος κοινωνιολόγος Edwin Sutherland. Σύμφωνα με τον Sutherland, πρόκειται για μία κατηγορία εγκλημάτων που λαμβάνουν χώρα στο πλαίσιο της επαγγελματικής δραστηριότητας του δράστη, ο οποίος φέρει τα εξής δύο βασικά χαρακτηριστικά: α) το υψηλό κοινωνικό status και β) η παράνομη πράξη που διαπράττεται αφορά την επαγγελματική του δραστηριότητα ή είναι σχετική με τα επαγγελματικά του καθήκοντα, όπως για παράδειγμα σε περιπτώσεις υπεξαιρέσεων, οικονομικών απατών κ.λπ. (Φαρσεδάκης, 2005).

Ως οικονομικό έγκλημα δεν θα πρέπει να θεωρείται οποιαδήποτε πράξη αποβλέπει σε όφελος οικονομικής φύσεως. Η ειδοποιός διαφορά ενός κοινού εγκλήματος με οικονομικό περιεχόμενο ή οικονομική ζημία με ένα οικονομικό έγκλημα έγκειται στο γεγονός ότι το δεύτερο κάνει την εμφάνιση του ως απόρροια της χρήσης και διαχείρισης των μηχανισμών του οικονομικού συστήματος προς όφελος του δράστη. Ουσιαστικά προσβάλλεται η εύρυθμη λειτουργία του οικονομικού συστήματος, ενώ το μέγεθος της ζημίας είναι πολύ μεγάλο. Συχνά είναι τόσο μεγάλο που μπορεί να συμπαρασύρει ολόκληρα υποσυστήματα της οικονομίας, όπως το χρηματοπιστωτικό σύστημα, το ασφαλιστικό ή το σύστημα της κεφαλαιαγοράς. Έτσι, τα θύματα ενός οικονομικού εγκλήματος, αυτό δεν περιορίζονται μόνο στα φυσικά πρόσωπα. Αντίθετα, ένα οικονομικό έγκλημα ενδέχεται να προσβάλλει κοινωνικά και έννομα αγαθά, κοινωνικές αξίες, το φυσικό περιβάλλον, συλλογικές οργανώσεις, επιχειρήσεις, το κράτος, κ.ο.κ (Περπέρης, 2015).

Σχετικά με το ηλεκτρονικό έγκλημα αφορά στη χρήση ηλεκτρονικών μέσων επικοινωνίας για εγκληματικές δραστηριότητες που περιλαμβάνουν ή στις οποίες εμπλέκεται το διαδίκτυο, καθώς και πληροφορίες ή τεχνολογία που βασίζονται σε αυτό. Το ηλεκτρονικό έγκλημα αποτελεί κάθε δραστηριότητα στην οποία διαμεσολαβεί η χρήση υπολογιστή ή άλλων σύγχρονων τεχνολογικών μέσων, διενεργείται μέσω παγκόσμιων ηλεκτρονικών δικτύων και έχει οριστεί ως παράνομη (Mc Lauhlin & Muncie, 2001). Η πληροφορική τεχνολογία κατέστησε δυνατή τη διάπραξη ενός ευρύτατου φάσματος εγκληματικών πράξεων, οι οποίες χαρακτηρίζονται από μεγάλη εξειδίκευση και αυξημένη κατάρτιση.

Τα τελευταία χρόνια, κυρίως από τη δεκαετία του 1980 και μετά, έχει κάνει την εμφάνιση της μια νέα μορφή οικονομικής εγκληματικότητας. Όταν η επέμβαση κάποιου τρίτου σε υπολογιστή έχει ως αποτέλεσμα, εκτός των άλλων, και την προσβολή έννομων αγαθών που έχουν φύση οικονομική, τότε μπορούμε, συνήθως να μιλάμε για ηλεκτρονικό-οικονομικό

έγκλημα. Το διαδίκτυο, μάλιστα, μπορεί να θεωρηθεί πλέον ως ένας τόπος άνθησης των οικονομικών εγκλημάτων (Wall, 2007). Από τεχνικής απόψεως, τα περισσότερα από τα οικονομικά εγκλήματα, σήμερα, μπορούν επίσης να ταξινομηθούν ως κυβερνοεγκλήματα, εφόσον οι δράστες συχνά εκμεταλλεύονται τις δυνατότητες του διαδικτύου για τη διάπραξή τους. Κατά τους McGuire και Dowling, η απάτη και η κλοπή είναι τα εγκλήματα που διευκολύνονται μέσω του διαδικτύου, όπως είναι οι διαδικτυακές τραπεζικές απάτες, οι απάτες μαζικού μάρκετινγκ, οι απάτες καταναλωτών, το ηλεκτρονικό ψάρεμα, κ. ά. (McGuire & Dowling, 2013, σύμφωνα με Jung & Lee, 2017). Είναι, λοιπόν, φανερό ότι η αλληλεξάρτηση του οικονομικού και του ηλεκτρονικού εγκλήματος είναι τόσο ισχυρή, που συχνά η διάκριση μεταξύ απλού ηλεκτρονικού και απλού οικονομικού εγκλήματος καθίσταται εξαιρετικά δυσχερής, με συνέπεια τη δημιουργία μιας νέας κατηγορίας, του «ηλεκτρονικού-οικονομικού εγκλήματος».

2. Ηλεκτρονικό-οικονομικό έγκλημα: Ηλεκτρονικές απάτες

Η διευρυμένη χρήση του διαδικτύου έχει επιφέρει και την αντίστοιχη αύξηση των εγκλημάτων που σχετίζονται με αυτό. Παρά το γεγονός ότι πλήττονται πολλά και διαφορετικά έννομα αγαθά, όπως για παράδειγμα το απόρρητο επικοινωνιών, τα προσωπικά δεδομένα, τα πνευματικά δικαιώματα κ.ο.κ, εντούτοις, δεν θα ήταν υπερβολικό να πούμε ότι ο πυρήνας των ηλεκτρονικών εγκλημάτων αποτελείται κυρίως από οικονομικά εγκλήματα. Σε αυτό το σημείο, οφείλουμε να σημειώσουμε ότι παρά την πληθώρα οικονομικών εγκλημάτων, στο παρόν θα αναλύσουμε ορισμένες από τις βασικότερες μορφές ηλεκτρονικής απάτης.

Ένα από τα συνηθέστερα οικονομικά εγκλήματα που τελούνται με τη βοήθεια των νέων τεχνολογιών είναι η απάτη με υπολογιστή. Οι πιο σύγχρονες μορφές ηλεκτρονικής απάτης συνδέονται άμεσα με την ευρεία χρήση του διαδικτύου και συνδυάζονται με τη χρήση πιστωτικών καρτών

και του e-banking, γνωστές με τους όρους ως «phishing» και «pharming». Κατά την διαδικασία του phishing, το θύμα λαμβάνει μια ηλεκτρονική επιστολή, η οποία υποτίθεται πως προέρχεται από το τμήμα ασφαλείας, διοίκησης ή μηχανογράφησης κάποιας τράπεζας, στην οποία καλείται να απαντήσει άμεσα, αποστέλλοντας τα στοιχεία της πιστωτικής κάρτας ή του τραπεζικού του λογαριασμού, για τις δήθεν ανάγκες αναβάθμισης λογισμικού, συστήματος ασφαλείας, κλπ. Πολύ συχνά χρησιμοποιούνται λογότυπα τραπεζών ή ακόμα τα ονόματα πραγματικών προσώπων που εργάζονται σε διοικητικές θέσεις στην τράπεζα, με στόχο να φαίνεται έγκυρη η εν λόγω επιστολή. Κατ' αυτό τον τρόπο, οι δράστες αποκτούν πρόσβαση στα προσωπικά δεδομένα του θύματος, με συνέπεια τη ζημίωση της περιουσίας, που ήταν και ο αρχικός στόχος (Κουράκης, 2007).

Μια ιδιαίτερη και πιο εξελιγμένη μορφή του phishing αποτελεί το λεγόμενο pharming, κατά το οποίο ο δράστης αντί να πείσει το θύμα όπως στην πρώτη περίπτωση, χρησιμοποιεί διάφορα προγράμματα που ανακατανέμουν ή αναδρομολογούν την κυκλοφορία των δεδομένων. Παρεμβαίνοντας στο λογισμικό του υπολογιστή, ο χρήστης – θύμα που θέλει να πραγματοποιήσει κάποια συναλλαγή κατευθύνεται, χωρίς να το γνωρίζει, σε ιστοσελίδα που αποτελεί αντίγραφο της γνήσιας. Τα στοιχεία, λοιπόν, που καταχωρούνται σε αυτό τον ιστότοπο, στην ουσία, βρίσκονται στη διάθεση του δράστη. Σε άλλες πάλι περιπτώσεις, αποστέλλονται μέσω ηλεκτρονικού ταχυδρομείου από το δράστη προγράμματα, τα οποία όταν εγκατασταθούν συλλέγουν και αποστέλλουν τα στοιχεία που ενδιαφέρουν το δράστη (όπως PIN, κωδικούς πρόσβασης κλπ.) , με αποτέλεσμα και πάλι την περιουσιακή ζημία του θύματος (Κουράκης, 2007).

Δεν είναι λίγες οι φορές που κατά την διαδικασία του phishing ή pharming συμμετέχουν και τρίτα πρόσωπα, με την ιδιότητα του ενδιάμεσου μεταξύ θύματος και δράστη. Ο δράστης, αφού εξασφαλίσει τα στοιχεία του λογαριασμού του θύματος και τους απαραίτητους κωδικούς πρόσβασης, επιχειρεί την να ζημιώσει την περιουσία του. Για να μην γίνει αντιληπτός

από τις αρχές, χρησιμοποιεί τρίτα πρόσωπα, γνωστά ως «οικονομικοί διαχειριστές» (finance managers), με τα οποία συνάπτει συμφωνίες (Moore et al. 2009).

Ακόμη, ιδιαιτέρως διαδεδομένες μορφές ηλεκτρονικής απάτης είναι οι απάτες διαδικτυακών δημοπρασιών και ηλεκτρονικού εμπορίου. Όσον αφορά τις απάτες διαδικτυακών δημοπρασιών, η διαδικασία δεν διαφέρει ιδιαίτερα από εκείνη των κλασικών δημοπρασιών. Οι πιθανοί αγοραστές και πωλητές ζητούν ή προσφέρουν μέσω των διαδικτυακών δημοπρασιών κάθε είδος αντικειμένων. Μετά την κατοχύρωση του αντικειμένου ο αγοραστής καλείται να αποστείλει την αξία του. Η απάτη λαμβάνει χώρα όταν το θύμα δε λαμβάνει ποτέ το αντικείμενο που έχει αγοράσει ή όταν του παραδίδεται ένα διαφορετικό ή μικρότερης αξίας αντικείμενο. Κάτι αντίστοιχο συμβαίνει και στις περιπτώσεις απάτης ηλεκτρονικού εμπορίου. Ο καταναλωτής δεν λαμβάνει ποτέ τα αγαθά που έχει παραγγείλει, ενώ συχνά γίνεται χρήση των προσωπικών του δεδομένων από τρίτους, χωρίς τη γνώση ή συγκατάθεση του, για οποιοδήποτε σκοπό (Περπέρης, 2015).

Συν τοις άλλοις, το διαδίκτυο παρέχει εύκολη και παγκόσμιας εμβέλειας πρόσβαση σε χώρους τυχερών παιγνίων, όπως είναι τα κλασικά παιχνίδια casino, λοταρίες, αθλητικά στοιχήματα και αγωνιστικά στοιχήματα. Τα τυχερά παιχνίδια στο διαδίκτυο αφορούν τη δραστηριότητα στο κυβερνοχώρο, ατόμων που παίζουν κάποιο παιχνίδι με το στοιχείο της τύχης - διακινδύνευσης ή στοιχηματίζουν έναντι κάποιου τιμήματος, με στόχο ένα μεγάλο οικονομικό όφελος (Banks, 2012). Το στοιχείο της απάτης υπεισέρχεται όταν υπάρχει παραπλάνηση ως προς την παρουσίαση των πιθανοτήτων να κερδηθεί ένα μεγαλύτερο χρηματικό ποσό ή των γεγονότων του παιχνιδιού. Οι παραπλανητικές ιστοσελίδες τυχερών παιγνίων εξαπατούν με «στημένα» ή «πειραγμένα» παιχνίδια, και τα κέρδη που προσφέρουν είτε δεν είναι προσβάσιμα στο νικητή, είτε δεν αποστέλλονται ποτέ. Έτσι, παράνομα θα χαρακτηρίζαμε τα τυχερά παιχνίδια στο διαδίκτυο, τα οποία είτε δεν πληρούν τις προϋποθέσεις, ως

προς την τοποθεσία τους , λαμβάνουν , δηλαδή, χώρα σε ιστότοπους που απαγορεύεται ο τζόγος, είτε επειδή αποτελούν τη βιτρίνα, πίσω από την οποία, κρύβονται εγκληματικές δραστηριότητες, όπως το ξέπλυμα χρήματος (Banks, 2012).

3. Η αντιμετώπιση του ηλεκτρονικού-οικονομικού εγκλήματος σε θεσμικό πλαίσιο

Στη διεθνή πραγματικότητα φαίνεται να επικρατούν τρεις τάσεις για την αντιμετώπιση της ηλεκτρονικής-οικονομικής εγκληματικότητας. Το ηλεκτρονικό-οικονομικό έγκλημα είτε αντιμετωπίζεται με το ισχύον νομοθετικό πλαίσιο ενός κράτους, με έννοιες που ερμηνεύονται κατά περίπτωση, είτε με νομοθετήματα που σχεδιάζονται ειδικά για τα ηλεκτρονικά εγκλήματα αλλά εντάσσονται στο ευρύτερο νομοθετικό πλαίσιο. Τέλος, η τρίτη τάση υπαγορεύει τη δημιουργία νόμων που θεσπίζονται για τη συνολική αντιμετώπιση του ηλεκτρονικού εγκλήματος και των επιμέρους μορφών του.

Ο παγκόσμιος και διακρατικός χαρακτήρας του ηλεκτρονικού εγκλήματος ολοένα και διογκώνεται, γεγονός που συνεπάγεται την απαίτηση για διεθνή συντονισμό αρχών και φορέων για την επιτυχή αντιμετώπιση του. Σε αυτό το σημείο θα κάνουμε αναφορά σε μερικές από τις σημαντικότερες διεθνής δράσεις για την αντιμετώπιση των ηλεκτρονικών-οικονομικών εγκλημάτων.

Σημαντική πρωτοβουλία αποτελεί η Συνθήκη της Βουδαπέστης του Συμβουλίου της Ευρώπης. Πρόκειται για την πρώτη συνθήκη αφιερωμένη στο ηλεκτρονικό έγκλημα. Υπογράφηκε το Νοέμβριο του 2001, ενώ τέθηκε σε ισχύ από τον Ιούλιο του 2004. Με γνώμονα την κάλυψη των νομικών κενών των εθνικών νομοθεσιών, η Συνθήκη της Βουδαπέστης, προωθεί το συντονισμό και συνεργασία αρχών και δράσεων, μέσω ευρωπαϊκών θεσμών όπως η Europol, για τη διερεύνηση και δίωξη του ηλεκτρονικού εγκλήματος.

Επιπλέον, προωθεί το συνδυασμό παραδοσιακών και πιο εξελιγμένων μορφών συνεργασίας μέσω διαύλων επικοινωνίας και αλληλοϋποστήριξης σε πραγματικό χρόνο (COE).

Σημαντική στον τομέα της πρόληψης και καταπολέμησης του ηλεκτρονικού εγκλήματος είναι και η συμβολή του ΟΟΣΑ. Από το 1997 και έπειτα, πέρα από ζητήματα οικονομικής φύσεως, εστιάζει και στην καταπολέμηση του κυβερνοεγκλήματος, εκδίδοντας κατευθυντήριες γραμμές σχετικά με τις τεχνολογίες κρυπτογράφησης και τονίζοντας την ανάγκη ύπαρξης ισορροπίας μεταξύ ιδιωτικότητας και εφαρμογής του κοινωνικού ελέγχου (Broadhurst, 2006).

Ακόμη, το 2015 των Ηνωμένων Εθνών (UNODC) και στο πλαίσιο της Επιτροπής για την Πρόληψη του Εγκλήματος και την Ποινική Δικαιοσύνη (CCPCJ), ξεκίνησε το Αποθετήριο Κυβερνοεγκλημάτων (Cybercrime Repository). Πρόκειται για μια κεντρική βάση δεδομένων νομοθεσίας, νομολογίας και ηλεκτρονικών αποδεικτικών στοιχείων σχετικών με το κυβερνοέγκλημα. Στόχος του Αποθετηρίου είναι να βοηθήσει τις χώρες στις προσπάθειές τους να αποτρέψουν και να διώξουν αποτελεσματικά τους δράστες εγκλημάτων στον κυβερνοχώρο (UNODC).

Στην ελληνική νομοθεσία τα ηλεκτρονικά-οικονομικά εγκλήματα εντάσσονται, συνήθως, κατά περίπτωση στα άρθρα 386 Α και 370 Β του ποινικού κώδικα, τα οποία αφορούν την απάτη με υπολογιστή και την παράνομη αντιγραφή και διείσδυση σε συστήματα και επικοινωνίες υπολογιστών, αντίστοιχα. Επιπλέον, τα ηλεκτρονικά-οικονομικά εγκλήματα αντιμετωπίζονται από την Υπηρεσία Οικονομικής Αστυνομίας και τη Δίωξη του Ηλεκτρονικού Εγκλήματος στην εδρεύει και το τμήμα Ειδικών Υποθέσεων και Δίωξης Διαδικτυακών οικονομικών εγκλημάτων. Κύριες αρμοδιότητες του τμήματος είναι η καταπολέμηση των οικονομικών εγκλημάτων, που τελούνται, κυρίως, στο πλαίσιο του διαδικτύου μέσω νέων τεχνολογιών και άλλων ηλεκτρονικών μέσων, σε βάρος των οικονομικών συμφερόντων του Δημοσίου και της εθνικής οικονομίας, ή

εγκλήματα που φέρουν τα χαρακτηριστικά της οργανωμένης εγκληματικότητας (Ελληνική Αστυνομία).

Επίλογος

Η διευρυμένη χρήση των ηλεκτρονικών υπολογιστών και του διαδικτύου έχει οδηγήσει και στην αντίστοιχη αύξηση των ηλεκτρονικών οικονομικών εγκλημάτων. Το ηλεκτρονικό οικονομικό έγκλημα, καθημερινά, διογκώνεται και επεκτείνεται σε νέους τομείς του κοινωνικού γίγνεσθαι. Θα μπορούσαμε να πούμε ότι το ηλεκτρονικό-οικονομικό έγκλημα, στην πλειονότητα των περιπτώσεων, αποτελεί ένα κοινό, «παραδοσιακό» οικονομικό έγκλημα, όπως είναι η απάτη, του οποίου η διάπραξη διευκολύνεται και απλουστεύεται με τη χρήση της σύγχρονης τεχνολογίας, και έχει ως τόπο τέλεσης, κυρίως, το περιβάλλον του διαδικτύου. Ωστόσο, λόγω της ιδιομορφίας του ηλεκτρονικού εγκλήματος, γενικά, και του ηλεκτρονικού οικονομικού εγκλήματος, ειδικότερα, παρατηρούνται ορισμένες δυσχέρειες στον τομέα της ποινικής αντιμετώπισης. Πολλά από τα αδικήματα είτε παραμένουν αρρύθμιστα, είτε εμπίπτουν στο ρυθμιστικό πεδίο περισσότερων ποινικών κανόνων. Αυτό έχει ως αποτέλεσμα να καθίσταται αναγκαία η παρέμβαση υπερκρατικών οργανισμών μέσω συμβάσεων, έκδοση οδηγιών και κατευθυντήριων γραμμών ή τη χρήση άλλων θεσμικών εργαλείων, με στόχο την ευθυγράμμιση των επιμέρους εθνικών νομοθεσιών προς την ίδια νομοθετική κατεύθυνση.

Βιβλιογραφία

Banks, J. (2012). «Online gambling and crime: a sure bet?», The ETHICOMP Journal, διαθέσιμο εδώ, ανακτήθηκε την 22/11/2020.

Broadhurst, R. (2006). «Developments in the global law enforcement of cyber-crime», *Policing: An International Journal of Police Strategies and Management*, 29 (3), σελ. 408-433.

COE (Council of Europe). «Details of Treaty No.185: Convention on Cybercrime», διαθέσιμο εδώ, ανακτήθηκε την 23/11/2020.

Ελληνική Αστυνομία, «Λειτουργία και αρμοδιότητες των τμημάτων της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος», διαθέσιμο εδώ, ανακτήθηκε την 23/11/2020.

Jung, J. & Lee, J. (2017). «Contemporary financial crime», *Journal of Public Administration and Governance*, 7 (2), σελ. 88-97.

Κουράκης, Ν. (2007). *Τα οικονομικά εγκλήματα ΙΙ: ειδικό μέρος*, Εκδόσεις Σάκκουλα.

Λάζος, Γ. (2004). *Οικονομική Εγκληματικότητα ΙΙ*, Σημειώσεις, Πάντειο Πανεπιστήμιο.

Mc Lauhlin, E. & Muncie, J. (2001), «Cybercrime», *The Sage Dictionary of Criminology*, σελ. 77-78.

Moore, T., Clayton, R. & Anderson, R. (2009). «The Economics of Online Crime», *Journal of Economic Perspectives*, 23 (3), σελ. 3-20.

Περπέρης, Α. (2015). *Το ηλεκτρονικό-οικονομικό έγκλημα: Ερευνητική προσέγγιση*, Διδακτορική διατριβή, Αθήνα: Πάντειο Πανεπιστήμιο.

UNODC. «Cybercrime repository», διαθέσιμο εδώ ανακτήθηκε την 23/11/2020.

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge: Polity.

Φαρσεδάκης, Ι. (2005). *Στοιχεία εγκληματολογίας*, Αθήνα: Νομική Βιβλιοθήκη.